FAS TURNITIN

by Apri Siswanto

Submission date: 24-Jun-2022 09:59PM (UTC+0700)
Submission ID: 1862340715
File name: cation_In_Smart_Home_Environment_Based_On_Embedded_turnitin.docx (1.09M)
Word count: 2591
Character count: 14583

Proc. of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)
16-18 November 2022, Maldives

Fingerprint Authentication In Smart Home Environment Based On Embedded System

***Abstract*— The concept of a "smart home" across the security field has increased significantly recently. One area of concern is the use of biometric fingerprint technology for authentication systems, such as authentication for entry to the home. This study designed a fingerprint authentication system based on fingerprints and PINs in a smart home environment. The hardware consists of an Arduino Mega 2560 as a microcontroller and an input/output supply. In addition, there is also a fingerprint sensor, and this component is used to capture the fingerprints of users. Based on the hardware design, the study determined implementation costs for authentication systems with fingerprints and PINs in an embedded system environment with lower implementation costs. It shows how to use a simple application to connect a door lock, fingerprint sensor, Arduino microcontroller, number keypad, and door lock.**

Keywords—fingerprint, authentication, security, embedded system, smart home

I. INTRODUCTION (*HEADING 1*)

In a smart home environment, user information needs protection to improve security identity management and authentication methods. However, conventional technologies, such as identification (ID) cards and personal identification numbers (PINs), are less reliable because they can be misplaced, forgotten, copied, forged, or misused. Therefore, it is inadequate to secure identity management and user authentication methods. Hence, the need for robust security practices is increasing. One of the practices is a fingerprint authentication system (FAS).

FAS is more secure than an ID card or PIN [1], where fingerprints have sixteen characteristics to distinguish each person, while a PIN only consists of a few numbers. FAS also provides excellent accuracy and speed to become a more reliable and precise solution for user authentication and identity management [2]. A fingerprint system is a commonly used technology for user authentication and access control devices. It can control access in offices, banks, factories, hospitals, universities, homes, e-commerce, cell phones, personal systems, and others. This system can be implemented in an embedded system, combining hardware and software for specific functions in a particular device [3]. The system consists of a microcontroller, fingerprint sensor, secure access control, and human interface. In a FAS, users' fingerprint information, known as fingerprint template (FT), is stored in the embedded device.

FAS can be divided into two main processes: (1) enrolment and (2) authentication. During the enrolment process, users' FT is registered and stored in a database, while the enrolment phase compares and verifies users' FT with the one stored in the database. In the process of enrolment, the fingerprint will be used as an identifier. Afterward, a sensor acquires data, and an algorithm processes them to extract fingerprint characteristics (i.e., templates). Finally, the template is stored in local or remote storage for future comparisons. Once the enrolment has been completed, the users are authenticated through the following steps: 1) reading the fingerprint, 2) extracting characteristics, and 3) comparing one by one with the previously stored template [4].

Fingerprint information or FT must be protected to ensure that only authorized users can access offices, banks, factories, hospitals, universities, smart homes, e-commerce, cell phones, personal systems, and others. Therefore, identity theft could be avoided while preventing replay attacks, stolen-verifier attacks, and perfect forward secrecy [5]. The most significant attack in FAS is the replacement of FT by impostors to gain unauthorized access. Therefore, fingerprint template protection (FTP) is needed to access offices, banks, factories, hospitals, universities, smart homes, e-commerce, cell phones, and personal systems to improve security in both enrolment and authentication for personal fingerprint protection.

According to Jain, et al. [6], the FTP scheme protects the user's fingerprint template and identities various biometric system vulnerabilities from leakage of biometric template information, leading to severe security and privacy threats. Wong, et al. [7] also said that FTP is a way to avoid the FT from being compromised, to experience permanent privacy and security issues. Other than that, Stanko, et al. [8] argued that FTP scheme is a technique for privacy-preserving storage of fingerprint data. In line with this argument, Mwema, et al. [9] said that FTP scheme is a technique used to secure biometric systems against these attacks. In short, FTP scheme is a generalized and efficient method to preserve privacy and to enhance the security of fingerprint authentication by limiting the exposure of FT data, which cannot be revoked. Although there are many studies that showed improvements in FTP schemes, there are still many open issues that need to be resolved by researchers [10]. Most importantly, FTP schemes have different requirements depending on their applications' domain. Unlike other applications' domains, user authentication in the embedded system operates on resource-constraint devices.

II. BIOMETRICS IN EMBEDDED SYSTEM

Biometrics have been implemented in many embedded systems [11, 12]. Alilla, et al. [13], Danese, et al. [14], Nie, et al. [15], Shinde and Bendre [16] and Dahal [17] present the implementation of biometrics in an embedded system based on microcontroller and field-programmable gate array (FPGA). However, biometric data encryption is not achieved in any FPGA implementation. Some research related to fingerprint authentication and embedded systems is presented in Table 1.

TABLE I. RESEARCH ON FINGERPRINT AUTHENTICATION SYSTEM

References	Embedded type	Highlights	Biometric
Nayak [18]	32-bit RISC microprocessor	The research proposed a fingerprint sensor that integrates sensors and 32-bit RISC microprocessors in a single chip. In addition, it presents an advanced detection circuit for processing capacitive fingerprint sensor signals and an effective isolation structure to remove any Electrostatic Discharge (ESD) effect.	Fingerprint
Militello, et al. [19]	FPGA	This study proposed embedded fingerprint authentication based on core and 10 singularity points. The proposed approach is divided into two parts: extraction and matching the singularity of algorithm points.	
Nie, et al. [15]	FPGA	This research proposed a multilevel fingerprinting method for FPGA IP protection	Fingerprint
Murillo-Escobar, et al. [20]	Freescale	This research proposed an FTP based on the chaos-based encryption algorithm.	Fingerprint
Martin, et al. [21]		The research proposed a global schema for fingerprint authentication with Arduino and fingerprint reader, a database server and monitoring mobile applications via smartphone. However, there is no encryption process in data transmission.	Fingerprint
García Vargas, et al. [22]	PIC18f252	This study proposed a portable and efficient fingerprint authentication system. The system employs an optical fingerprint sensor with an embedded microcontroller that performs effective image processing.	Fingerprint

The embedded system is based on software and hardware, which uses processors with limited computing power, limited memory, and input-output devices. The system's advantages are low cost, small physical size, low power consumption, high performance, and flexibility [20]. In other words, an embedded FAS with a template security interface can help to reduce the risk of fraud and identity theft. An embedded expert system has an "intelligence" capacity to perform fingerprint enrolment and verification with security guarantees, low cost, high performance, template protection guaranteed, store data, and transmit it over unsecured channels [20]. This system can potentially be used as access control in an embedded system environment or smart offices. Embedded systems are designed for the specific purpose of performing one or many tasks in real-time computing. The characteristics of this system are [23] :

1. designed in one integrated device between one component and other components in a microcontroller.
2. designed to perform specific tasks and not for general tasks.
3. software for this system is generally in the form of firmware, which is the software to communicate and interact in real-time with hardware.

Fingerprint templates can be imitated or modified so that legal users cannot access the legal system environment and compromise the system's security. Then, the attackers illegally access and modify the system later. In addition, they can change the access rights of authorized users [26]. FT can be modified or replicated because FTP schemes are also vulnerable to various systems that exploit insecure system infrastructures, such as replay attacks and denial of service attacks (see Figure 1). There are also loopholes or insider attacks [27].

Additional vulnerabilities from the FTP scheme are related to people's ability to identify fingerprint patterns based on fingerprints obtained from an object touched and limited liveness-detection capabilities of conventional FTP systems. FTP system is an architecture of fingerprint authentication, indicating its significant vulnerabilities and its four underlying causes, as shown in Figure 1. It is not difficult to make spoof fingerprints from fingerprints images or even a stored FT and get unauthorized access. This system is also vulnerable to intrinsic failure (also known as zero-effort attacks), which leads to incorrect authentication. Finally, it is due to limited individuality and intra-class fingerprint features that need to be secured by the FTP algorithm so that data integrity can be maintained properly.

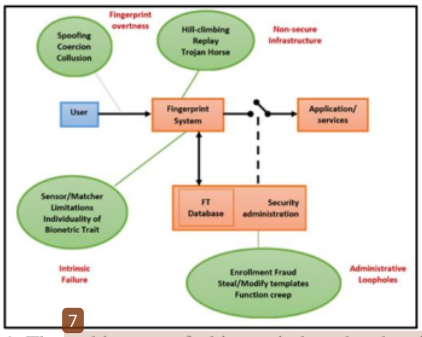

Figure 1. The architecture of a biometric-based authentication system indicates its major vulnerabilities and their four underlying causes [27]

Fingerprint refers to the lines that appear on the skin of the fingertips. The fingerprint works to give a more significant frictional force for the finger to hold objects closer [28]. The reason for choosing fingerprint in this study is because it is highly distinctive and unique to every person, even identical twins [29]. Then, fingerprint authentication is the most extensive and reliable mechanism for individual identification [30]. It is also usually accessible, reliable, and highly accurate [31]. It has been widely used in various fields, including attendance systems, immigration, home building access, etc. A fingerprint is an ultimate choice for excellence as a biometric identifier. It has long been employed for recognition

purposes. The reliability and superiority of fingerprints in authentication systems have gone beyond other types of biometrics such as faces or irises [32]. At the same time, due to the decreasing cost and size of fingerprint sensors, it is very prospective that fingerprint continues to be widely used in biometric recognition systems in the future. Indeed, the recent biometric market report, a summary in the Wall Street Journal, estimates that FAS will continue to dominate the biometric market in the future.

III. DESIGNING FAS IN A SMART HOME ENVIRONMENT

The FAS was implemented on a hardware module that included a 32-bit microcontroller, fingerprint sensor, networking tool, and human interface. In the enrolment process, the user can register the FT by using minutiae extraction to generate the user's FT. Then, the FT is sent to the microcontroller through the transmission line and stored in the microcontroller's flash memory. For the verification, users' FT will be compared to the FT stored in the database to authenticate the users. The hardware design is illustrated in Figure 2.

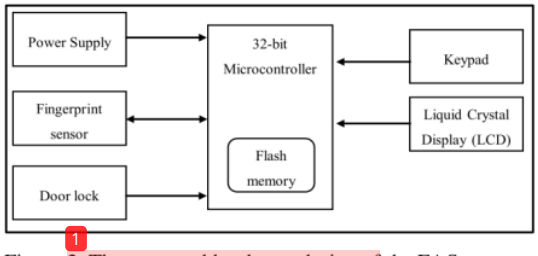

Figure 2. The proposed hardware design of the FAS

The materials used in this study are divided into two categories hardware and software. Hardware material refers to concrete equipment used in the study, such as Personal Computer (PC), fingerprint optic sensor, microcontroller, door lock, LCD and power supply. Software materials are substances that could not be seen or touched. They are virtual objects used in application development. Software applications include Arduino integrated development environment (IDE), and C programming language.

IV. RESULT AND DISCUSSION

Fingerprint sensors control the smart home's main entrance and garage door. When this system is installed at home, authorized homeowners must use a simple application to register their fingerprint data, which is then stored in the Arduino microcontroller memory. Residents enter their PINs and use the fingerprint sensor to scan their fingerprints. In Arduino memory, the scan results are kept in digital format. Then, fingerprint records are analyzed to generate a list of distinct feature features. A database stores the fingerprint pattern feature. Residents' fingerprint patterns will be changed to match those in the database when they scan their fingertips. If the two data sets are identical, the Arduino memory sends an approval signal to the microcontroller, allowing the residents to unlock the door lock/electric latch. Figure 3 depicts the prototype that was produced.

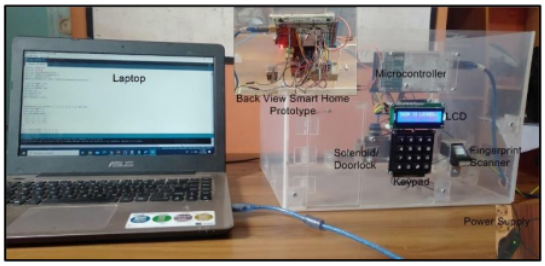

Figure 3. Hardware prototype design

A user must register his fingerprint in a smart home system for it to be recognized in the Arduino Mega 2560 microcontroller database during the fingerprint user enrollment process. The following are the steps in the registration procedure. The user first enters their PIN and then scans their fingerprint. The user must then place their finger again to guarantee that the fingerprint model is formed. The user will be able to access the smart home that has been constructed using the user's fingerprint or PIN registered in the database after the fingerprint data has been successfully recorded into the database. The fingerprint enrolment method for smart house door lock security is depicted in Figure 4.

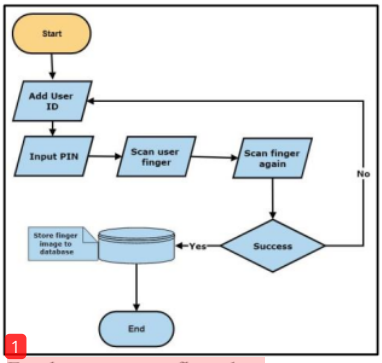

Figure 4. Enrolment process flow chart

There are three steps to handling the smart home prototype enrolment process. The first is the display process in the embedded smart-home system when deciding whether to add, delete, open, or exit. For example, to add a new user, press the "Add" button and then enter the new user's PIN. The fingerprint data will be registered in the smart home system once you place your finger on the sensor twice. As illustrated in Figure 5, the prototype was created in an embedded smart home environment.

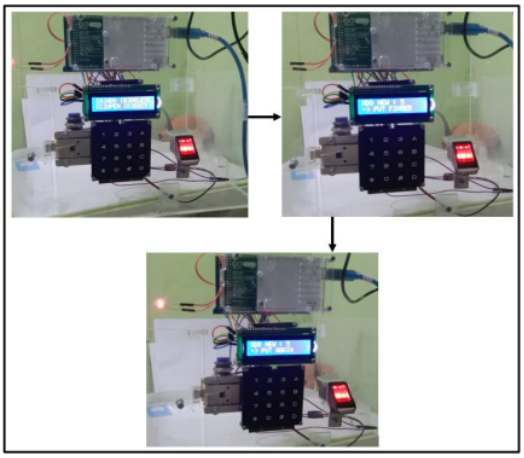

Figure 5. Enrolment process in prototype smart home

The user fingerprint template that has been registered in the system will be able to access the prototype of the smart home environment after being successfully recorded into the database. The user places their finger on a fingerprint sensor and scans it. The system will check to see if the data model matches the database. The door/solenoid will open if it is proper, but it will be refused if it is not. If the sensor cannot read the fingerprint data owing to filthy or injured hardware or fingers, the user can enter the door using the PIN that has been stored in the database. The system is also designed to handle the homeowner's request to delete a user. Figure 6 depicts the flow chart of the prototype system that was constructed.

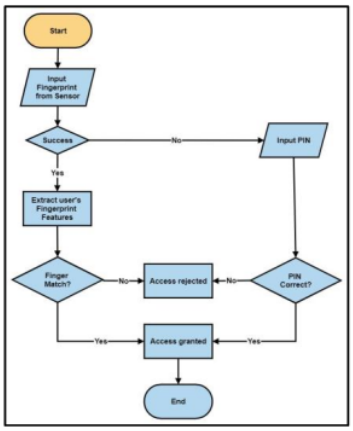

Figure 6. Authentication process flow chart

Currently, authentication techniques rely on smart cards, which will inevitably result in a slew of security issues if smart cards are lost. Using the proposed fingerprint system or PIN protocol to authenticate could overcome security issues created by stolen or lost smart cards. Figure 7 depicts the authentication process in the smart home prototype.

Figure 7. The authentication process in the prototype

The LCD will display the words "access denied", and the solenoid will still lock if the fingerprint pattern reading is invalid and the user is not registered in the system database.

Based on testing with numerous user fingerprints, this prototype appears capable of performing well in the database's enrolment and authentication processes. The testing of user fingerprint prototypes in the smart home setting is shown in Table 2. The user creates a PIN and scans their fingerprints twice during enrolment. On the table, fingerprints are used instead of a PIN for authentication. The proposed FAS takes 3.5 seconds to enroll and 2 seconds to authenticate. However, if the fingerprint sensors fail or the user's finger becomes wounded (dirty) and no longer works to enter or unlock doors in the home, the user can use a PIN to gain access to the smart home system.

V. CONCLUSION

This study designed a fingerprint authentication system based on fingerprints and PINs in a smart home environment. The proposed fingerprint authentication protocol is secure and more efficient for the authentication system in a smart home environment. It consists of user enrolment and authentication phases. A prototype of a fingerprint smart home authentication provides a basic overview of integrating a door lock, fingerprint sensor, Arduino microcontroller, number keypad, and door lock with a simple application.

FAS TURNITIN

ORIGINALITY REPORT

24%	4%	22%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Apri Siswanto, Akmar Efendi, Zalian Hasrin, Bustamil Arifin. "Chapter 18 Two-Factor Authentication for Safe Deposit Box Based on Embedded System", Springer Science and Business Media LLC, 2022 Publication	13%
2	M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez. "A robust embedded biometric authentication system based on fingerprint and chaotic encryption", Expert Systems with Applications, 2015 Publication	5%
3	www.semanticscholar.org Internet Source	1%
4	ijece.iaescore.com Internet Source	1%
5	Submitted to Rajiv Gandhi Proudyogiki Vishwavidyalaya Student Paper	1%

6	Submitted to Institute of Research & Postgraduate Studies, Universiti Kuala Lumpur Student Paper	1 %
7	Submitted to South Bank University Student Paper	1 %
8	repository.dkut.ac.ke:8080 Internet Source	<1 %
9	www.inettutor.com Internet Source	<1 %
10	Ahmet Anil Mungen, Mehmet Kaya. "Features and Connection Based Network Alignment Method", 2019 International Artificial Intelligence and Data Processing Symposium (IDAP), 2019 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		